

## IN THE CLAIMS

1       1.       (previously presented) A method for updating a program in a data processing  
2       system comprising the steps of:  
3               requesting a trusted platform module ("TPM") to perform a signature  
4       verification of an update to the program;  
5               the TPM performing the signature verification of the update to the program;  
6               if the signature verification of the update to the program is successful, using  
7       the TPM for unlocking a memory unit storing the program; and  
8               modifying the program with the update to the program in response to the  
9       unlocking of the memory unit storing the program.

1       2.       (original) The method as recited in claim 1, further comprising the step of:  
2       locking the memory unit after the modifying step.

1       3.       (original) The method as recited in claim 2, wherein the locking step is  
2       performed by the TPM.

1       4.       (previously presented) A computer program product for storage on a  
2       computer readable medium and operable for updating a BIOS stored in a flash  
3       memory in a data processing system, comprising:  
4               a BIOS update application program receiving an updated BIOS image;  
5               the BIOS update application requesting a TPM to perform a signature  
6       verification of the updated BIOS image;  
7               a TPM program receiving the request from the BIOS update application to  
8       perform the signature verification of the updated BIOS image;  
9               the TPM program performing the signature verification of the updated BIOS  
10       image and posting a result of the signature verification of the updated BIOS image to  
11       the BIOS update application;

1           if the result of the signature verification of the updated BIOS image  
2 determines that the updated BIOS image is authentic, then the TPM program unlocks  
3 the flash memory; and

4           the BIOS update application modifies the BIOS with the updated BIOS image.

5.       (cancelled)

1       6.       (previously presented) The computer program product as recited in claim 4,  
2 further comprising:

3           programming for locking the flash memory after the BIOS update application  
4 modifies the BIOS with the updated BIOS image.

1       7.       (original) The computer program product as recited in claim 6, further  
2 comprising:

3           if the result of the signature verification of the updated BIOS image  
4 determines that the updated BIOS image is not authentic, then an error message is  
5 output.

1       8.       (original) A data processing system having circuitry for updating a BIOS  
2 stored in a flash memory in the data processing system, comprising:

3           input circuitry for receiving an updated BIOS image;  
4           circuitry for requesting a TPM to perform a signature verification of the  
5 updated BIOS image;  
6           the TPM performing the signature verification of the updated BIOS image;  
7           the TPM unlocking the flash memory if the signature verification of the  
8 updated BIOS image determines that the updated BIOS image is authentic; and  
9           circuitry for modifying the BIOS with the updated BIOS image.

1       9.       (original) The system as recited in claim 8, further comprising:  
2               circuitry for locking the flash memory after the BIOS is modified with the  
3       updated BIOS image.

1       10.      (original) The system as recited in claim 8, further comprising:  
2               circuitry for outputting an error if the signature verification of the updated  
3       BIOS image determines that the updated BIOS image is not authentic.